Reflection

The Network and Information Security Management (NISM) module was taught over twelve weeks and focused on the theoretical paradigms including security concepts and key terms as well as practical aspects of network technology. The majority of the assignments were conducted in a team of five students though there were individual tasks too.

As part of the module, we had to discuss and agree on our team's rules and procedures for the team contract such as rotation of the Team Leader position and individual participation. It was great to see how each team member contributed and participated. Over the twelve weeks, it became evident that the initial excitement and willingness started to deteriorate, and members positioned themselves into certain roles and expectations which had profound consequences on an individual, team, and academic level for the rest of the term; the team settled into a dynamic of leaders and followers.

The module was organised into weekly units focusing on different aspects of NISM such as DREAD analysis and a GDPR case study. Each unit followed a logical approach of reading research articles, industry blogs, and chapters from cyber security textbooks, attending biweekly seminars and lecture casts. This was underpinned by three forum discussions which allowed classmates to post their viewpoints and respond to comments on key NISM topics. We were tasked to record our NISM learning journey on our individual GitHub ePortfolio in a structured and logical way which had the added benefit of using GitHub Markup and HTML.

Regarding assessments, we had two team assignments on discovering vulnerabilities of a website using cyber security industry tools namely Kali Linux and presenting learned evidence in the ePortfolio.

I was slightly apprehensive when starting this module than the previous Launching into Cyber Security module due to the more complex nature of NISM and the group work element. I really enjoyed the practical and technical aspect of configuring and deploying Kali Linux tools such as OWASP ZAP and Nmap; and seeing the scanned results highlight vulnerabilities and potential exploits of the website. Curiously, learning and studying government regulations and industry standards; for example, GDPR and ISO 27000 was quite interesting as this allowed me to better understand the greater impact NISM and cyber security has on society in terms of being responsible for the protection of personal data and IT systems and related infrastructure.

It seems my experience of group work was mixed bag of joy and despair. Although we managed to submit our projects in advance of the deadline, this was negated by intragroup dynamics especially group roles. Initially when the group was in the ‘get to know each other’ phase, we had a seminar presentation on the DREAD analysis. I had already prepared an outline and shared it with the group along with my thoughts which resulted in ideas being discussed and added.

However, no one was willing to present at the seminar, so I decided to do it. This set a precedent throughout the module. Another team member and I became the de facto leaders which meant tasks and activities were coordinated, planned, and democratic.

Despite this, I felt that this was unfair as it meant we had to collate, prepare, proofread, edit the team's projects as the other team members refused to offer or take the role as outlined in the Team Contract. Furthermore, I also presented three of our group's seminar tasks when the role should have been rotated.

On reflection, I realised that I was part of the problem. My eagerness to instigate and be pro-active for the seminar task solidified my group position as a 'leader'; however, the reluctance of other team members to share or participate in the role or work led to inequality within the group resulting in my low self-esteem. This is mirrored by McCauley (1998) who posits low temporary self-esteem is a result of recent failures, difficulties in current decision-making, and moral dilemmas.

These concerns were shared by the other team member, and we both agreed the added pressure and workload was unjust; nevertheless, it motivated us to complete the tasks in the best possible manner to achieve a successful outcome.

Overall, I learned how to gather information on potential threats to and vulnerabilities of a website and report it to the owners. By reading beginner manuals of Kali Linux and penetration testing tools, I learned how to configure and become a moderately proficient user of Kali Linux and its penetration tools. This allows me to practise my newly found skills on my home and friends' networks. I am a more informed on industry regulations and standards, and I am more confident in discussing NISM topics in a more in-depth manner. Conversely, I realise my group did not function as effectively as I hoped, and this contributed to the projects and tasks not being to the high standard I expected. If I were to do group work again, I would ask each member about their strengths and weaknesses as this would help to understand each member better as well as foster better team cohesion.

References

McCauley, C. (1998) Group Dynamics in Janis's Theory of Groupthink: Backward and Forward. *Organizational Behavior and Human Decision Processes*, 73(2-3), pp.142–162. doi:10.1006/obhd.1998.2759.